UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/754,018	01/03/2001	Motoshi Ito	YAMAP0748US	3434

7590 01/12/2007

Neil A. DuChez
Renner, Otto, Boisselle, & Sklar, L.L.P.
19th Floor
1621 Euclid Avenue
Cleveland, OH 44115

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/754,018	ITO ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 10/19/2006.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 10/19/2006 have been fully considered but they are not persuasive.

Regarding the applicants' argument that the cited references do not teach a portion of the single hardware circuit performing both a data scramble function and an error correction function, the examiner does not find the argument persuasive. First, the examiner notes that with regards to claim 1, the details of the circuit have not been given patentable weight, as the claim is directed towards the control program and not the circuit.

Second, the examiner further notes that as the claims are presented, a logical box around the decryption and error correction elements of Oishi still meets the newly recited claim limitation of "a portion" performing both functions. As claimed, the limitation is still a "logical" box wherein both functions are performed. Further still, the claim does not appear to be consistent with the specification in that the specification discloses a specific function (the 8-order primitive polynomial) which happens to scramble the data input for error correction, and the claim merely claims any circuit which performs both error correction and data scrambling. As such, the examiner does not find the argument persuasive.

Further note the new rejection in view of Murakami et al. presented below.

All objections and rejections not presented below have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1, 3, and 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirotani (US Patent Number 5,982,887), further in view of Oishi (US Patent Number 6,907,125), and further in view of Schneier (Applied Cryptography), and further in view of Elabd (US Patent Number 6,526,462).

Regarding claim 1, Hirotani disclosed a control program for controlling an operation of a microprocessor (See Hirotani Col. 4 Paragraph 3), the control program comprising a concealed program (See Hirotani Col. 3 Paragraph 7), recoverable by data scramble circuit (See Hirotani Col. 3 Paragraph 8) and a non-concealed program (See Hirotani Fig. 1 Element 15 wherein only part of the program is encrypted). However, Hirotani failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani also fails to disclose the use of a system on a chip design.

Oishi teaches that in order to protect against errors in a decryption system, error correction can be combined with the decryption system by encrypting error correction codes as well as the stored data and then decrypting the codes and using the codes in error correction (See Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product.

Regarding claim 3, Hirotani disclosed a device, comprising: a microprocessor (See Hirotani Fig. 3 Element 21), a program memory for storing a control program for controlling an operation of the microprocessor (See Hirotani Fig. 3 Element 25), the control program including a concealed program (Element 25 Encrypted Section) and a non-concealed program (Element 25 Program section); a rewritable memory for storing a copy of the concealed program copied from the concealed program stored in the program memory (See Hirotani Col. 6 Paragraph 2 and the

rejection of claim 1 above wherein it was inherent that the encrypted program was stored, at least temporarily in a rewritable memory in the decryption circuit, before decryption), and a data scramble circuit for recovering the concealed program stored in the rewritable memory as a recovered program (See Hirotani Col. 6 Paragraphs 2-3 and the rejection of claim 1 above), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function.

Oishi teaches that in order to protect against errors in a decryption system, error correction can be combined with the decryption system by encrypting error correction codes as well as the stored data and then decrypting the codes and using the codes in error correction (See Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the

CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product.

Regarding claim 6, Hirotani disclosed a method for creating a control program, comprising: a program descramble step of descrambling a portion of a control program by reverse scramble of a data scramble circuit in a device to be controlled, thereby creating a concealed program as a portion of the control program (it was inherent in the invention of Hirotani that a portion of the control program was encrypted in order for the control program to have taken on the form of Element 25 in Fig. 3); and a program storing step of storing the control program including the concealed program in a program memory so that the control program controls an operation of a microprocessor in the device to be controlled (See Hirotani Col. 5 lines 39-44), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function.

Oishi teaches that in order to protect against errors in a decryption system, error correction can be combined with the decryption system by encrypting error correction codes as well as the stored data and then decrypting the codes and using the codes in error correction (See Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product.

Regarding claim 8, Hirotani disclosed a method for operating a control program, comprising: a program copying step of copying a concealed program which is a portion of the control program (See Hirotani Fig. 3 Element 25) from a program memory into a rewritable memory (See rejection of claim 3 above); a program recovery step of recovering the concealed program copied by the program copying step as a recovered program by a data scramble circuit (See rejection of claim 3 above); and a program execution step of executing a non-concealed program included in the control program and the recovered program (See Hirotani Col. 6 Paragraph 5), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function.

Oishi teaches that in order to protect against errors in a decryption system, error correction can be combined with the decryption system by encrypting error correction codes as well as the stored data and then decrypting the codes and using the codes in error correction (See Oishi Col. 3 Paragraph 4 and Col. 4 – Col. 6 Line 23)

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oishi and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Oishi for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product.

Regarding claim 7, the combination of Hirotani, Oishi, Schneier, and Elabd disclosed that the program descramble step includes the steps of: creating a non-concealed program (it was

inherent that the program was created at some point in order for the program to have been encrypted and downloaded); and synthesizing the concealed program and the non-concealed program into the control program (See Hirotani Fig. 3 Element 25 wherein the encrypted and non-encrypted programs are together as the program stored in program memory).

Regarding claim 9, the combination of Hirotani, Oishi, Schneier, and Elabd disclosed a program erasure step of erasing the recovered program from the rewritable memory (See Hirotani Col. 6 Paragraph 6).

Claims 2, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Hirotani, Oishi, Schneier, and Elabd as applied to claims 1 and 3 respectively above, and further in view of Oualline ("Practical C++ Programming") and Ooi et al. (U.S. Patent Number 5,226,129) hereinafter referred to as Ooi.

The combination of Hirotani, Oishi, Schneier, and Elabd disclosed a recoverable encrypted program to be run on a microprocessor (See rejection of claim 1 above) but Hirotani failed to disclose the composition of the program as well as the addressing mode of the program. However, Hirotani did disclose that the encrypted program could have been downloaded over a network (See Hirotani Col. 3 Lines 27-29).

Oualline teaches that in order to conserve memory space, commonly used code can be grouped into functions such that the code can be used repeatedly (See Oualline Page 133 Paragraph 1). Ooi teaches that in order to easily make a program portable, the program should use relative addressing (See Ooi Col. 1 Lines 27-33).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oualline to create functions in the encrypted program of

Hirotani, Oishi, Schneier, and Elabd. This would have been obvious because the ordinary person skilled in the art would have been motivated to make the program as compact as possible in order to conserve memory and also to limit the amount of information needing to be transferred over the network to the system of Hirotani. It further would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Ooi in the program of Hirotani, Oishi, and Schneier by providing the program with relative addressing. This would have been obvious because the ordinary person skilled in the art would have been motivated to minimize the modification of the code required to relocate the program, and thus increase portability.

It would have been obvious in the combination of Hirotani, Oishi, Schneier, Elabd, Oualline, and Ooi that relative address lists for the functions of the program would be provided in the program at prescribed, or predetermined, location, in order for the processor of Hirotani to be able to locate the functions called throughout the program.

Claims 1, 3, and 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirotani (US Patent Number 5,982,887), further in view of Murakami et al. (US Patent Number 5,613,005) hereinafter referred to as Murakami, and further in view of Schneier (Applied Cryptography), and further in view of Elabd (US Patent Number 6,526,462).

Regarding claim 1, Hirotani disclosed a control program for controlling an operation of a microprocessor (See Hirotani Col. 4 Paragraph 3), the control program comprising a concealed program (See Hirotani Col. 3 Paragraph 7), recoverable by data scramble circuit (See Hirotani Col. 3 Paragraph 8) and a non-concealed program (See Hirotani Fig. 1 Element 15 wherein only

part of the program is encrypted). However, Hirotani failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function. Hirotani also fails to disclose the use of a system on a chip design.

Murakami teaches a particular encryption and decryption circuit which uses irreducible polynomials which corrects errors during decryption in order to protect against errors or missing data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Murakami and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product.

Regarding claim 3, Hirotani disclosed a device, comprising: a microprocessor (See Hirotani Fig. 3 Element 21), a program memory for storing a control program for controlling an operation of the microprocessor (See Hirotani Fig. 3 Element 25), the control program including a concealed program (Element 25 Encrypted Section) and a non-concealed program (Element 25 Program section); a rewritable memory for storing a copy of the concealed program copied from the concealed program stored in the program memory (See Hirotani Col. 6 Paragraph 2 and the rejection of claim 1 above wherein it was inherent that the encrypted program was stored, at least temporarily in a rewritable memory in the decryption circuit, before decryption), and a data scramble circuit for recovering the concealed program stored in the rewritable memory as a recovered program (See Hirotani Col. 6 Paragraphs 2-3 and the rejection of claim 1 above), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function.

Murakami teaches a particular encryption and decryption circuit which uses irreducible polynomials which corrects errors during decryption in order to protect against errors or missing data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Murakami and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of

Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product.

Regarding claim 6, Hirotani disclosed a method for creating a control program, comprising: a program descramble step of descrambling a portion of a control program by reverse scramble of a data scramble circuit in a device to be controlled, thereby creating a concealed program as a portion of the control program (it was inherent in the invention of Hirotani that a portion of the control program was encrypted in order for the control program to have taken on the form of Element 25 in Fig. 3); and a program storing step of storing the control program including the concealed program in a program memory so that the control program controls an operation of a microprocessor in the device to be controlled (See Hirotani Col. 5 lines 39-44), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function.

Murakami teaches a particular encryption and decryption circuit which uses irreducible polynomials which corrects errors during decryption in order to protect against errors or missing data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Murakami and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product.

Regarding claim 8, Hirotani disclosed a method for operating a control program, comprising: a program copying step of copying a concealed program which is a portion of the control program (See Hirotani Fig. 3 Element 25) from a program memory into a rewritable memory (See rejection of claim 3 above); a program recovery step of recovering the concealed program copied by the program copying step as a recovered program by a data scramble circuit (See rejection of claim 3 above); and a program execution step of executing a non-concealed

program included in the control program and the recovered program (See Hirotani Col. 6 Paragraph 5), but failed to disclose that at least a portion of the data scramble circuit is operative to perform both a data scramble function and an error correction function.

Murakami teaches a particular encryption and decryption circuit which uses irreducible polynomials which corrects errors during decryption in order to protect against errors or missing data in a decryption system, (See Murakami Col. 1 Line 57 – Col. 2 Line 7).

Schneier teaches that encryption and decryption can be performed in a hardware circuit (See Schneier Pages 223-225).

Elabd teaches that instead of using a traditional, separate component integrated circuit design, a system on chip design can be used (See Elabd Col. 1 Lines 20-59).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Murakami and Schneier in the decryption system of Hirotani by utilizing the decryption/error correction system of Murakami for the decryption of Hirotani and further by providing a hardware decryption circuit to be used in place of the CPU decryption. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the integrity of the program in a cost efficient manner, and further would have been motivated to increase the speed of the decryption, increase the security of the decryption, ease in the installation of the decryption method, and increase the efficiency of the CPU. Furthermore, it would have been obvious to utilize the teachings of Elabd in the system by providing the components of the system on a single chip. This would have obvious because the ordinary person skilled in the art would have been motivated to produce a smaller, faster, more efficient, and less expensive product.

Regarding claim 7, the combination of Hirotani, Murakami, Schneier, and Elabd disclosed that the program descramble step includes the steps of: creating a non-concealed program (it was inherent that the program was created at some point in order for the program to have been encrypted and downloaded); and synthesizing the concealed program and the non-concealed program into the control program (See Hirotani Fig. 3 Element 25 wherein the encrypted and non-encrypted programs are together as the program stored in program memory).

Regarding claim 9, the combination of Hirotani, Murakami, Schneier, and Elabd disclosed a program erasure step of erasing the recovered program from the rewritable memory (See Hirotani Col. 6 Paragraph 6).

Claims 2, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Hirotani, Murakami, Schneier, and Elabd disclosed as applied to claims 1 and 3 respectively above, and further in view of Oualline ("Practical C++ Programming") and Ooi et al. (U.S. Patent Number 5,226,129) hereinafter referred to as Ooi.

The combination of Hirotani, Murakami, Schneier, and Elabd disclosed a recoverable encrypted program to be run on a microprocessor (See rejection of claim 1 above) but Hirotani failed to disclose the composition of the program as well as the addressing mode of the program. However, Hirotani did disclose that the encrypted program could have been downloaded over a network (See Hirotani Col. 3 Lines 27-29).

Oualline teaches that in order to conserve memory space, commonly used code can be grouped into functions such that the code can be used repeatedly (See Oualline Page 133 Paragraph 1). Ooi teaches that in order to easily make a program portable, the program should use relative addressing (See Ooi Col. 1 Lines 27-33).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Oualline to create functions in the encrypted program of Hirotani, Murakami, Schneier, and Elabd. This would have been obvious because the ordinary person skilled in the art would have been motivated to make the program as compact as possible in order to conserve memory and also to limit the amount of information needing to be transferred over the network to the system of Hirotani. It further would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Ooi in the program of Hirotani, Murakami, and Schneier by providing the program with relative addressing. This would have been obvious because the ordinary person skilled in the art would have been motivated to minimize the modification of the code required to relocate the program, and thus increase portability.

It would have been obvious in the combination of Hirotani, Murakami, Schneier, Elabd, Oualline, and Ooi that relative address lists for the functions of the program would be provided in the program at prescribed, or predetermined, location, in order for the processor of Hirotani to be able to locate the functions called throughout the program.

Conclusion

Claims 1-3, and 5-9 have been rejected.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Matthew Henning
Assistant Examiner
Art Unit 2131
12/29/2006

Taghi T. Arani
Primary Examiner
Taghi T. Arani
1/7/07